AS4 thoughts for PEPPOL

Author: Philip Helger, BRZ, Austria

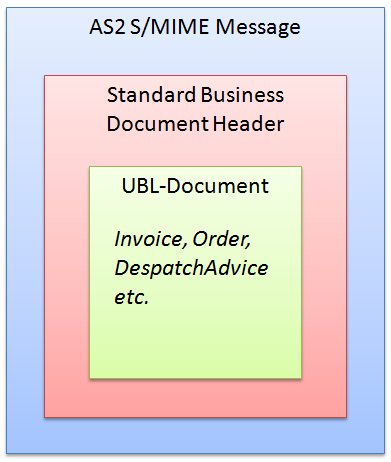
# Introduction

PEPPOL is most likely switching from AS2 to AS4 and this document contains some general thoughts on it.

# AS2

The AS2 solution is using the following features:

* Basically an S/MIME message
* Requires https transport (transport level encryption) – using non-PEPPOL certificates (!)
* Business documents (UBL/XML) are wrapped in SBDH (Standard Business Document Header)
* AS2 transmissions are signed with the PEPPOL AP certificates



# AS4

AS4 messages can be presented as SOAP messages with a single SOAP body or as MIME messages containing SOAP messages without a body (SOAP with attachments).

Message exchange patterns (MEP bindings) can be one of the following: push, pull, sync, push-push, push-pull, pull-push

# PEPPOL requirements

## Correlation with MLR and BLR

We would need something like “push-push-push”

* C2 🡪 C3 Document
* C3 🡪 C2 MLR (optional)
* C3 🡪 C2 BLR (optional)

# Mail Jose

I send you some questions to be discussed in Peppol AS4 document if you consider them useful.

* Pull and sync will be used?
* The Service Metadata Record provides also the receiving end's certificate. This certificate can be used for encrypting the message to be sent to C3 MSH and for that it must be mapped with the new created P-Mode. The certificate can also provide the name of the gateway for this P-Mode, by using the Certificate's CNAME as the P-Mode identifier. This approach has been used in the CIPA Implementation of dynamic P-Modes, in CIPA AP Version 2.4.2. Actually the certificate is only used to validate MDNs. Message ciphering will be used on AS4?

Trust and Security Concerns in Message Reception

The certificate that signed the message might not be known beforehand, so it is not in the trust store. An option is that the message contains the certificate and preferably the complete cert path. In that case the AS4 gateway might only need to contain the root CA certificate in its trust store to be able to validate the signature. Certificate recognition on incoming messages will still use certificate CN as APP and CA verification chain against OpenPeppol CA?

Also if you could point me to what you consider the most controversial points to discuss in AS4 Peppol profile I can read and extract conclusions for next meeting.